REMARKS

Reconsideration of the application is respectfully requested.

Claims 1-23 and 25-30, that are pending, have been examined and rejected as reported in the Office Action. The following addresses the rejections in the order they appear in the Office Action.

Claims 1-5, 7-8, 10-12, 15-22 and 26-28 stand rejected as being anticipated by U.S. Patent No. 5,918,047 issued to Leavitt, et al. ("Leavitt"). Applicants have amended claim 1 to overcome the rejection by reciting a system comprising a non-volatile data storage device *configured as one or more storage regions to store one or more bytes of CMOS BIOS data, wherein the device lacks hardware security such that some of the regions may be accessed by an application program in the system.* In addition, claim 1 as amended, recites that the system has *another non-volatile data storage device to store a mirror image of the CMOS BIOS data.* A program store has processor-readable instructions to ascertain the validity of the CMOS BIOS data and, if invalid to replace the data with the mirror image. Leavitt does not teach or suggest such a system.

In Leavitt, the problem is that initialization programs in the one-time programmable (OTP) ROM were defective, then successful initialization of the system was impossible until the OTP ROM was replaced. The solution presented in Leavitt is to test, for example, using a boot block code, a primary BIOS code block that has been loaded into flash memory. If the test passes, the code block is loaded into shadow RAM. If not, then an alternate code block is loaded from disk to shadow RAM and/or to the flash memory. However, Leavitt is only concerned with protection against system crashes caused by defective initialization programs, and does not teach or suggest the problem addressed by Applicants' claim 1 as amended here, where the computer system has **CMOS BIOS regions in a non-volatile storage device that lacks hardware security such that some of the CMOS BIOS regions are modifiable by an application program in the system.** The issue in Leavitt is not the lack of hardware security for CMOS BIOS, but rather how to deal with defective programs in OTP ROM, which, are not modifiable (unlike CMOS BIOS data) and do not present a security

concern. Accordingly, reconsideration and withdrawal of the rejection in view of Leavitt is respectfully requested.

Turning now to claim 10, this claim has been amended to more clearly recite an embodiment of Applicants' invention that is neither anticipated nor obvious. In this method, current CMOS BIOS content that is stored in a non-volatile storage device is read. In addition, a valid image of the CMOS BIOS content is also read, from a further non-volatile storage device. A determination is made as to whether the current content has been modified without authorization, and the current content is replaced with the stored valid image, if the current content is determined to have been modified without authorization. Leavitt does not teach or suggest such a system, because Leavitt is directed to a crash recovery mechanism (for boot code in OTP ROM) that does not concern itself with unauthorized modifications to inherently unprotected CMOS BIOS content. Accordingly, claim 10 as amended, is not anticipated or obvious in view of Leavitt.

Claim 17 recites a method that has been amended to refer to the arranging of a non-volatile storage device of a computer system into one or more storage regions to store CMOS BIOS data, wherein the device lacks hardware security such that some of the CMOS BIOS regions are modifiable by an application program in the system. An integrity metric corresponding to valid CMOS BIOS content that is stored in a first region of the device is generated, and the integrity metric is stored in another non-volatile storage device of the system, to later determine if the content in the first region has been modified without authorization.

Although Leavitt refers to non-volatile storage devices of a computer system having defective initialization code, Leavitt is only concerned with recovering from a system crash that may have been caused by the defective initialization code in a one-time programmable ROM. There is no hardware security concern with the boot code that is in the one-time programmable ROM, as the ROM is not modifiable. Although that boot code is later indicated as being stored in flash memory which is rewriteable, Leavitt fundamentally does not teach or suggest Applicants' claim 17, which is concerned with non-volatile devices that store CMOS BIOS data. Such devices lack hardware security and, therefore, expose some of the CMOS BIOS regions to

unauthorized modifications by an application program. Accordingly, reconsideration and withdrawal of the rejection of claim 17 in view of Leavitt is respectfully requested.

In claim 20, Applicants' method has been amended to once again refer to the arranging of a non-volatile storage device of a computer system into one or more storage regions to store CMOS BIOS data, where once again the device lacks hardware security such that some of the CMOS BIOS regions are modifiable by an application program in the system. The method includes comparing the current content in a first region to an earlier stored image of the content and replacing the current content that is stored in the first region of the non-volatile storage device, with the previously stored image, if it is determined that there has been unauthorized modification of the current content in the non-volatile storage device. The problem of unauthorized modification of CMOS BIOS data in a non-volatile storage device of a computer system is not taught or suggested in Leavitt.

Finally, claim 26 recites a machine-readable medium with instructions for protecting content in a non-volatile storage device that stores CMOS BIOS data against unauthorized modification (e.g., by an application program in the system). The medium includes instructions that cause a processor in the system to read current CMOS BIOS content stored in the non-volatile storage device, determine if the read content has been modified without authorization, and replacing the content with a previously stored image taken from a flash memory of the system. Leavitt does not teach or suggest such a system.

In Leavitt, there is a single flash memory 20 that stores BIOS code, but does not teach or suggest two separate non-volatile storage devices, where one is to store CMOS BIOS content and the other is to store an image of the CMOS BIOS content. According, reconsideration and withdrawal of the rejection in view of Leavitt is requested.

Any dependent claims not mentioned above are submitted as not being anticipated or obvious for at least the reasons given above in support of their base claims.

CONCLUSION

In sum, a good faith attempt has been made to explain why the rejection of the claims is improper in view of the relied upon art reference, and to correct obvious errors in the claims, without altering their scope. A Notice of Allowance referring to claims 1-22 and 26-30, as amended here, is therefore requested to be issued at the earliest possible date.

If necessary, the Commissioner is hereby authorized in this, concurrent and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17, particularly, extension of time fees.

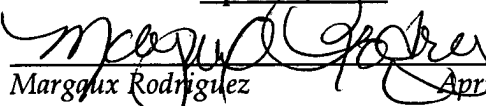Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR, & ZAFMAN LLP

Dated: <u>April 13, 2006</u>   By _____
Farzad E. Amini, Reg. No. 42,261

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, Post Office Box 1450, Alexandria, Virginia 22313-1450 on <u>April 13, 2006.</u>

_____
Margaux Rodriguez   *April 13, 2006*